Before the
Federal Communications Commission
Washington, D.C. 20554

FCC Public Notice	)	
	)	CC Docket No. 96-115
Privacy and Security of Information Stored	)	
On Mobile Communications Devices	)	

COMMENTS OF COMMON SENSE MEDIA

Common Sense Media ("Common Sense") is pleased to submit its comments in the Commission's above captioned proceeding concerning the issue of privacy and security of information as related to mobile devices, and the need for greater privacy protections for children and teens. Common Sense agrees with the Commission's observation that technologies and business practices in the telecommunications industry have evolved dramatically during the past few years and that §222 of the Communications Act of 1934, 47 U.S.C.§ 222(a), establishes a duty of carriers to "protect the confidentiality of proprietary information of, and relating to … customers."[1] The Commission should continue to update the protections of personal information under §222, especially for children and younger teens.

Common Sense is one of the nation's leading nonprofits dedicated to improving the media lives of kids and families. Through a free K-12 digital literacy and citizenship education curriculum now used in over 35,000 schools nationally, parent tips and reviews provided via the Commonsense.org web site, and advocacy on such issues as cyberbullying, privacy and digital citizenship, we seek to educate on how media can best impact the health and well-being of our nation's youth.

---

[1] *Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, 27 FCC Rcd 5743 (2012).

Carriers should provide additional protections of transparency, disclosure, informed consent, breach notification, and data security requirements for the information stored on mobile devices, particularly for younger customers. (1) Carriers should provide transparency by filing with the Commission their agreements with third parties and the details of their data collection and usage, explaining what information is being collected by carriers, and the circumstances under which information is shared with third parties; (2) Carriers should provide disclosure in a clear and conspicuous manner to consumers about the information they collect, use and share from users' mobile devices; (3) Carriers should obtain an informed opt-in consent before collecting, sharing and using information from users' mobile devices; (4) Carriers should provide adequate notice of any data breaches of information stored on mobile devices; and (5) the Commission, working with industry, should issue a set of data security requirements for information stored on mobile devices.

These protections are even more important in the case of young consumers. Common Sense Media's recent study, *Zero to Eight: Children's Media Use in America*[2] showed the high level of engagement that even very young children have with mobile devices:

- Half (52%) of all 0- to 8-year-olds now have access to smartphones or other newer mobile devices at home.
- More than a quarter (29%) of all parents have downloaded apps for their children to use.
- In a typical day, 11% of 0- to 8-year-olds use a cell phone, iPod, iPad or similar device and those who do spend an average of 43 minutes with the device.

Ironically, precisely at the moment in which younger customers have the freedom to utilize broadband mobile devices – often for very desirable reasons – these kids are most vulnerable to abuses of their personal information. All five members of the Commission

[2] Common Sense Media, ZERO TO EIGHT: CHILDREN'S MEDIA USE IN AMERICA (Fall 2011), available at http://www.commonsensemedia.org/sites/default/files/research/zerotoeightfinal2011.pdf.

acknowledged this recently when they said they would support an Internet privacy bill of rights for users under the age of 15.[3]

Consumers are better positioned to protect their personal information when they have control over their information and a meaningful understanding of what is being done with the information on their device. The task of privacy protection becomes more important as technologies converge. Proper disclosure, transparency and consumer choice are key in a converging world. It is particularly important for younger users to have the ability to protect their privacy by understanding what information being collected, stored and monitored by carriers and third parties.

At the same time, convergence creates yet more difficulties for carriers to manage the security of such information. This makes it ever more important for the FCC to work with industry to create a set of strong yet practical data security requirements.

As part of this evolution of privacy and changing technologies, the Commission in 2007 addressed the practice of pretexting. As noted in the FCC's Notice, Congress this year directed questions to several carriers concerning the use of "Carrier IQ" software to enhance network reporting capabilities and how mobile carriers are directing the collection and storage of customer specific information on devices.[4]

The Carrier IQ inquiry only highlights the need for the Commission to ensure the protection of CPNI-type information on consumers' mobile devices, especially for younger consumers. This enterprise will likely require placing additional responsibility on the shoulder of carriers. But this simply reflects the central role that carriers play in the collection and use of

[3] Haley Tsukuyama, *FCC commissioners say they would support an under-15 privacy bill of rights #thecircuit*, THE WASHINGTON POST, July 10, 2012, http://www.washingtonpost.com/blogs/post-tech/post/fcc-commissioners-say-they-would-support-an-under-15-privacy-bill-of-rights-thecircuit/2012/07/10/gJQAD78saW_blog.html.
[4] *Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, 27 FCC Rcd 5743, 5745 (2012).

consumer data. The carrier is the one contractually bound to the consumer (and is the one with the access and knowledge of the interconnected eco-system which provides these converged services via the mobile device), as well as often the party with the most robust interaction with mobile device users, including the parents of minor users. As a practical matter, the carrier is best positioned to help the customer protect his own information by allowing him full disclosure as to what information is being retained, transferred and monitored by the carrier (or by third parties if the carrier is aware of such usage).

Technological advances and new services should be encouraged. New innovations should not undercut traditionally protected privacy. Protecting consumers' information will ensure that commerce continues to flourish as consumers will feel confident to engage in commerce and communications with the understanding of how their data is being collected and stored.

Respectfully submitted,

Guilherme Roschke

Policy Counsel

July 13, 2012